Prof. Dr.-Ing. Peter Liggesmeyer

Die Vorstandsperspektive

Informatik ist in vielen klassischen Anwendungsbereichen, z. B. in Transportsystemen, in der Medizintechnik oder der Automatisierungstechnik, unverzichtbar. Software erbringt oft große Teile der Funktionalität. Software verursacht einerseits Risiken, bietet andererseits aber auch Chancen zu ihrer Beherrschung. In der Vorstandskolumne erläutert Prof. Dr.-Ing. Peter Liggesmeyer, Vizepräsident der Gesellschaft für Informatik e.V., diese Situation anhand des Beispiels „Zertifizierung von Schienenfahrzeugen“.

Informatik mit Sicherheit; Sicherheit mit Informatik

Im April 2013 druckte DIE WELT einen Artikel mit dem Titel: „Behörde schiebt 140 Züge aufs Abstellgleis; Bahnindustrie: Weil Zulassungen fehlen, verrotten fabrikneue Wagen auf Halden“. Gegenstand des Artikels ist das vermutete Spannungsfeld zwischen der Bahnindustrie und der in Deutschland zuständigen Zulassungsbehörde – dem Eisenbahnbundesamt (EBA).

Man darf sicherlich den Herstellern, den Betreibern und auch den Zulassungsbehörden unterstellen, dass sie ein gemeinsames Ziel verfolgen, und zwar die kostengünstige Bereitstellung eines komfortablen, sicheren, verfügbaren, zuverlässigen Verkehrsmittels. Und das sollte natürlich auch das Interesse der Nutzer – also der Bahnkunden – sein. Wir wollen bei der Benutzung eines Zuges gefahrlos und ohne Ausfälle unterwegs unser Ziel erreichen. Außerdem sollen die Fahrpreise nicht übermäßig hoch sein.

Zwischen den Kosten und den anderen genannten Eigenschaften wird man eine Wechselwirkung vermuten, nach dem Motto: „Gute Systeme kosten etwas mehr.“ Tatsächlich stehen aber auch Sicherheit, Verfügbarkeit und Zuverlässigkeit in Wechselwirkung, und das ist bei der Bahn besonders sichtbar, weil Bahnsysteme eben eine explizite Zulassung erfordern. Solange diese nicht erteilt ist, dürfen die betroffenen Systeme nicht betrieben werden und stehen – vermeintlich fertig – herum. Darüber, ob die Systeme aber wirklich fertig sind oder doch noch nicht ganz, kann man trefflich streiten. Um das zu verstehen, muss man die genannten Eigenschaften etwas detaillierter betrachten.

Selbstverständlich läuft die Zulassung eines Systems nicht rein nach dem Ermessen eines Gutachters ab. Das Verfahren fußt vielmehr auf einschlägigen Standards. Sicherheit in der hier verwendeten Ausprägung (sogen. Safety) wird sinngemäß in den entsprechenden Standards definiert als „die Abwesenheit unakzeptabel hoher Risiken“. Das bedeutet, dass ein restrisikobehaftetes System als sicher gelten kann, wenn diese Risiken als akzeptabel eingestuft werden. Systeme, die frei von Restrisiken sind, können nicht gebaut werden, bzw. es gibt keine Technik, mit der man sich vergewissern könnte, dass dies gelungen ist. Für die Zulassung eines Systems ist es erforderlich, die vorhandenen Risiken zu bestimmen und anschließend zu entscheiden, ob diese Risiken akzeptiert werden können oder Modifikationen nötig sind.

Moderne Züge sind komplizierte Artefakte, bei denen potenziell gefährliches Verhalten durch das Zusammenwirken von Software, Elektronik und maschinenbauerischen Komponenten zustande kommt. Das macht die Bestimmung der Risiken nicht einfacher, und Software hat daran ihren Anteil. Bahntechnikhersteller investieren erhebliche Ressourcen in den Zulassungsprozess. Man kann durchaus nachvollziehen, dass dies aus ihrer Perspektive betrachtet hin und wieder ein Ärgernis sein mag, sollte aber auch dankbar sein für die unabhängige Rolle des Eisenbahnbundesamts als „Wächter der Sicherheit“. Es ist die Pflicht einer Zulassungsbehörde, die aus ihrer Sicht erforderlichen Nachweise einzufordern, und es ist eine wohl natürliche Reaktion von Herstellern, die Forderung

bestimmter Nachweise gelegentlich als überzogen zu empfinden. Hier muss immer wieder ein Kompromiss gefunden werden.

Ein Kompromiss zwischen Eigenschaften ist aber auch an anderer Stelle notwendig. Es mag seltsam erscheinen, aber oft verursacht bei Schienenfahrzeugen und auch vielen anderen Systemen eine Verbesserung der Sicherheit eine Verringerung der Verfügbarkeit. Die in das Zugsystem eingebauten Diagnoseroutinen erkennen Ausfälle und reagieren wie vorherbestimmt. Es gibt dabei zwei gegensätzliche Möglichkeiten:

1. Die Diagnose ist „sensibel“. Zur Gefahrenabwehr wird das System im Zweifel in einen eigensicheren Zustand gebracht, was im Extremfall zu seiner Abschaltung führt. Er ist dann zwar sicher, arbeitet aber nicht, ist also nicht verfügbar.
2. Die Diagnose ist „unsensibel“. Die Wirkung von Ausfällen wird unterschätzt und das System wird einfach weiterbetrieben, dies allerdings möglicherweise in unsicherer Form. Es arbeitet, ist also verfügbar, aber evtl. nicht sicher.

Die Diagnosesoftware muss ganz offensichtlich einen guten Kompromiss finden. Sie darf weder überzogen pessimistisch, noch übertrieben optimistisch reagieren. Natürlich gibt es neben „Abschalten“ und „einfach weiterlaufen lassen“ noch eine dritte Option: „Umschalten“. Das setzt aber voraus, dass in dem System für die ausgefallene Komponente eine Reservekomponente existiert, also Redundanz verbaut ist. Das hat selbstverständlich Auswirkungen auf die Kosten. Man wird Redundanz also nur dort vorsehen, wo sie sich rentiert. Um das abschätzen zu können, ist ein genaues Verständnis von Wirkmechanismen nötig, das bei der Analyse der Restrisiken mit entsprechenden Techniken – quasi nebenher – entsteht.

Eine verbesserte Zuverlässigkeit steigert die Verfügbarkeit, weil ein System, das seltener ausfällt, natürlich öfter funktionsfähig anzutreffen ist.

Es gibt aber auch unzuverlässige Systeme mit hoher Verfügbarkeit, die zwar oft ausfallen, aber kurzfristig repariert werden können. Falls alle Ausfälle ungefährlich sein sollten, so kann ein System sogar tatsächlich gleichzeitig unzuverlässig und sicher sein. Derartige Systeme wird der Benutzer allerdings kaum akzeptieren.

Warum dieser Exkurs in die Zertifizierung von Bahntechnik im Informatik-Spektrum? Informatik spielt in diesem Bereich und in vielen ähnlichen Bereichen – etwa im Automobilbau, der Medizin- oder Automatisierungstechnik – heute eine zentrale Rolle. Software macht die Systeme komplizierter und erschwert so die Risikoanalyse; aber Software ist auch das wichtigste Mittel zur Realisierung intelligenter Lösungen für die Erkennung und den Umgang mit Ausfällen.

Man erwartet, dass Software in Zukunft sogar Teile der Zertifizierung bestimmter Systeme übernehmen könnte – vielleicht nicht gleich in so kritischen Bereichen wie der Bahntechnik. Wenn Systeme sich während der Laufzeit verändern, so muss das System selbst in der Lage sein, festzustellen, ob eine Modifikation erlaubt ist oder nicht, weil sich eine nicht akzeptable Kombination der System-Eigenschaften einstellen würde. Man bezeichnet das als „Zertifizierung zur Laufzeit“. Daran wird geforscht. Und natürlich wird das mit Hilfe geeigneter Software durchgeführt werden. Diese Software muss dann natürlich sehr hohe Qualitäts-Anforderungen erfüllen.

Hier gibt es viele Fragen. Um sie zu beantworten, braucht es smarte Informatik.

Prof. Dr.-Ing. Peter Liggesmeyer,
Vizepräsident der Gesellschaft für Informatik e.V.,
TU Kaiserslautern und Fraunhofer IESE,
peter.liggesmeyer@gi.de